Forward for the new edition of

“What Every Engineer Should Know About Risk Engineering and Management"

In aerospace and engineering in general, the major metrics are capability, cost, and safety/risk. With the increasingly rapid emergence and utilization of new technologies and systems of increasing complexity, ensuring safety becomes more difficult. The technology and practice/applications of safety/risk technologies require updating in concert with capability and systems technology changes. Hence the new, updated edition of this risk engineering book. Major changes in technology and applications, now and going forward, increasingly involve artificial intelligence (AI)/autonomy and complex systems, which are rapidly developing and moving targets when it comes to risk/safety analysis. These introduce both new risks and safety issues, and they alter more usual ones. The current reality is that often the best AI is when it is “Black Boxed”, developed “independently”, without detailed human understanding of how and by what processes decisions and results are produced. There are ongoing efforts to make the AI processes more understandable by humans, with results to be determined. Also, trusted and true autonomy is free of human intervention, which would require machines to ideate to solve in real time issues that arise due to unknown unknowns and even known unknowns. Machines using generative adversarial network (GANs) and other approaches are beginning to ideate. Overall, the capabilities and practice of AI/autonomy utilization is a work in progress with the rate of progress substantial and the impacts upon system risk/safety major.

As systems become more complex and have increasing numbers of piece parts, there are possibilities for cascading failures, where subcritical issues with one part can alter the functionality of other system piece parts and cause subcritical failures, contingent upon which/what/how the system is configured. Hence the need for serious risk/safety analyses at the system and system of systems level. In many systems/applications, software is both the most expensive and the most troublesome because of extant errors when installed and errors instilled during operation either by operators or by environmental effects. In many systems, human factors are major sources of error, including traffic accidents and in aerospace. Safety or risk issues in aerospace include rockets, whose safety record is an issue occurring every 100 launches or so, orders of magnitude more of a safety concern than the superb safety record of commercial aviation. There is now interest in certification by computation vice experiment. Unfortunately, the computations do not consider, nor have available, the detailed aspects of the as-built physical system.

Overall, safety/risk is not what it was in the Industrial Age, and as this book espouses, risk considerations now include a vast number of possible issues, with an increasing number of newer technologies and complexities

and assumptions, all of which can interact at the systems of system level. All of this is in the context of the increasing importance of cost, which puts a premium upon reducing “fail safe” redundancies and over-design as a whole. Risk assessment is both changing rapidly and becoming ever more difficult and critical to engineering success. Hence this updated edition.

Dennis M. Bushnell, HFAIAA, FASME, FRAeS
Chief Scientist, NASA Langley Research Center